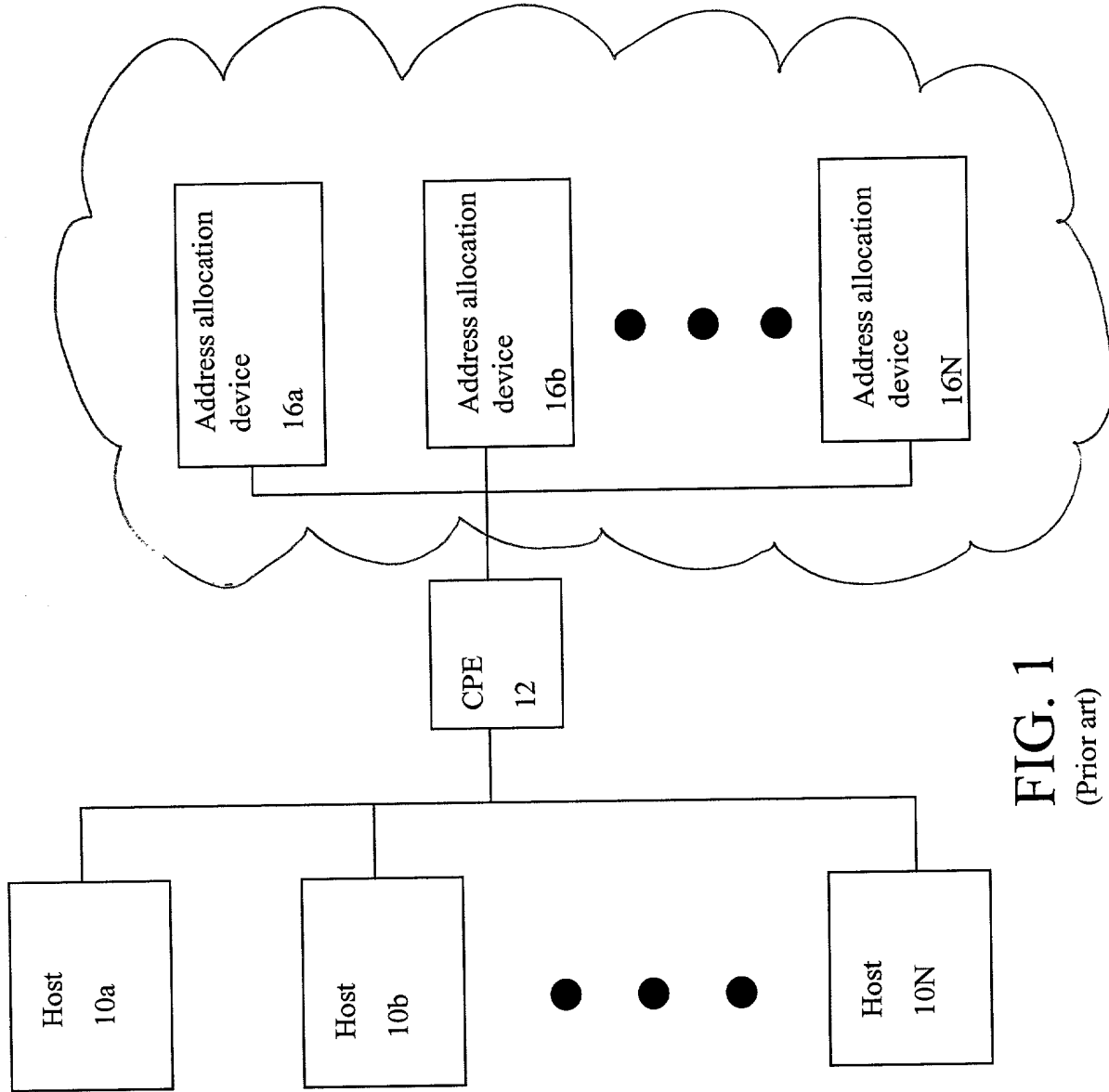


CISCO-3840



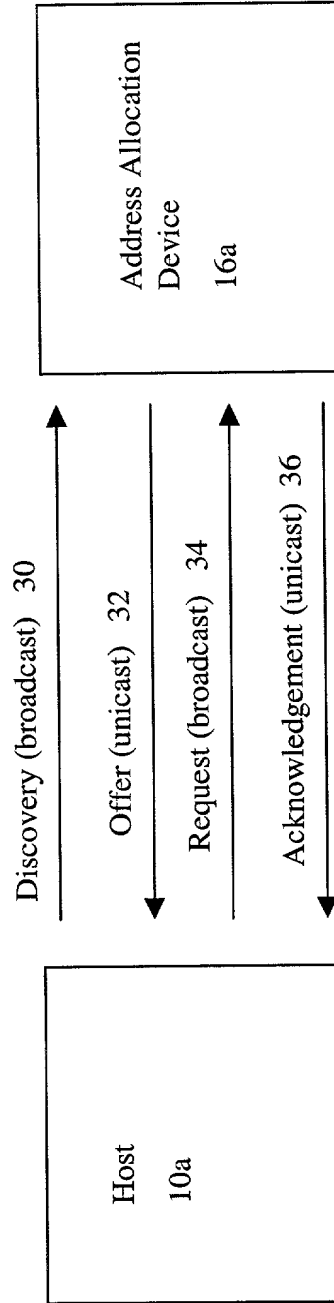
**FIG. 1**  
(Prior art)

CISCO-3840

|            |       |      |      |
|------------|-------|------|------|
| op 20      | htype | hlen | hops |
| xid        |       |      |      |
| secs       | flags |      |      |
| ciaddr 24  |       |      |      |
| yiaddr     |       |      |      |
| siaddr 22  |       |      |      |
| giaddr 26  |       |      |      |
| sname      |       |      |      |
| file       |       |      |      |
| options 18 |       |      |      |

FIG. 2  
(Prior art)

CISCO-3840



**FIG. 3**  
(Prior art)

CISCO-3840

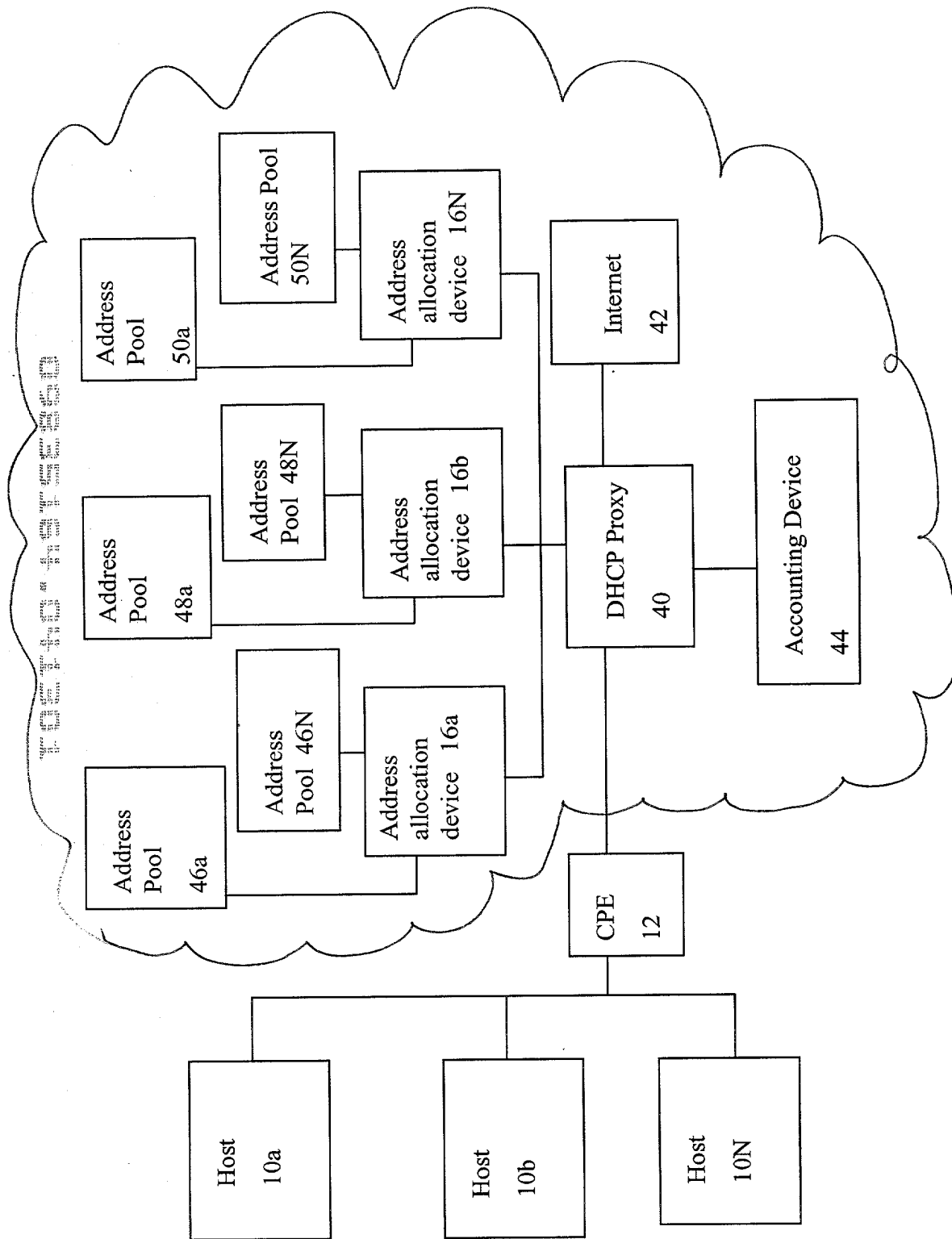


FIG. 4

CISCO-3840

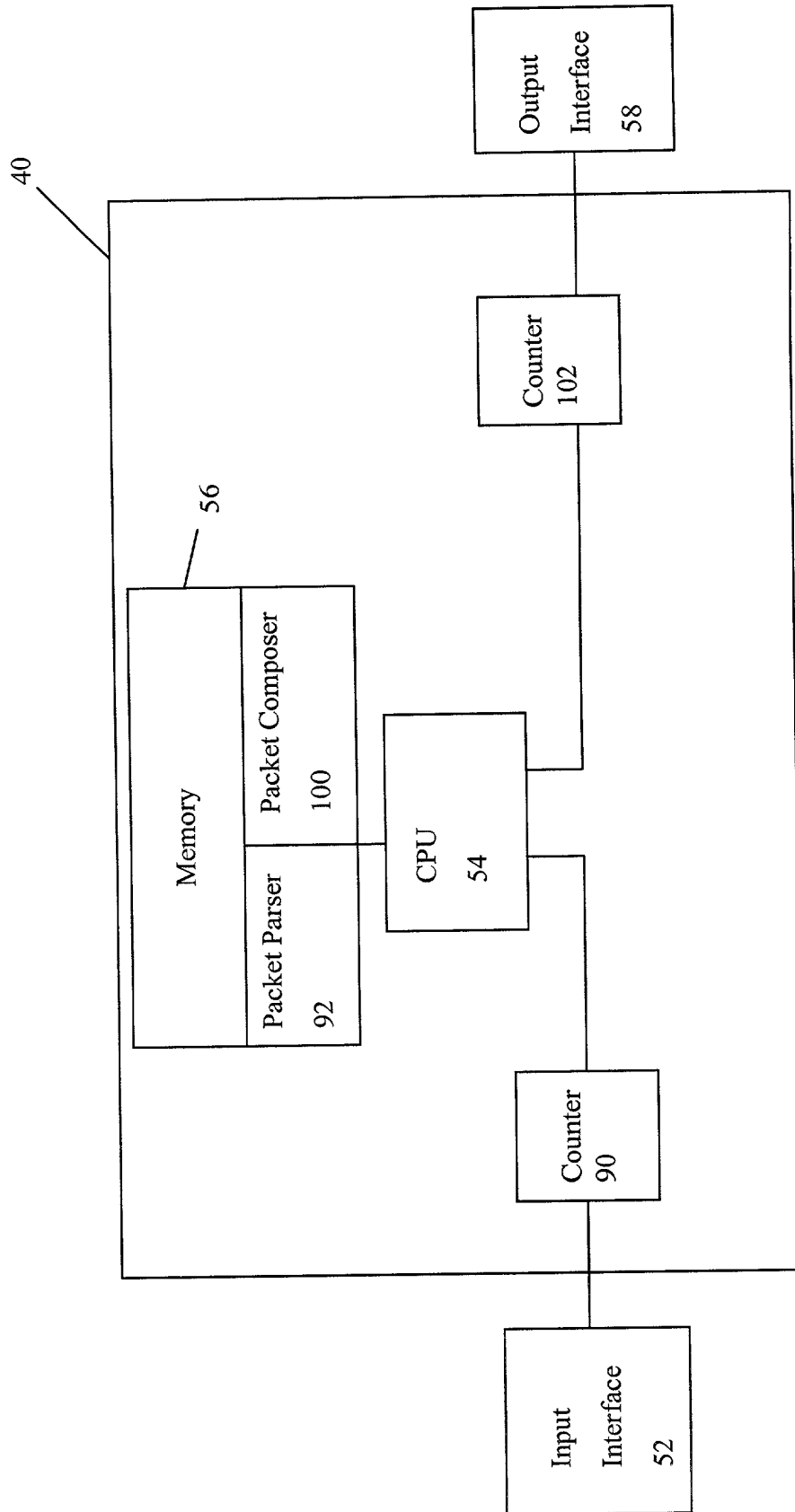


FIG. 5A

Cisco-3840

FIG. 5B is a block diagram of a system 40, such as a Cisco-3840, configured to perform the operations of the system 40 as described herein. The system 40 includes an input interface 52, a CPU 54, a memory 56, a counter 90, a counter 102, and an output interface 58. The memory 56 includes a packet parser 92 and a packet composer 100. The system 40 is configured to receive input data from the input interface 52, process the input data using the CPU 54 and the memory 56, and output the processed data to the output interface 58. The counter 90 is configured to count the number of packets received from the input interface 52, and the counter 102 is configured to count the number of packets sent to the output interface 58. The packet parser 92 is configured to parse the input data into packets, and the packet composer 100 is configured to compose the processed data into packets for output to the output interface 58. The system 40 is configured to perform the operations of the system 40 as described herein.

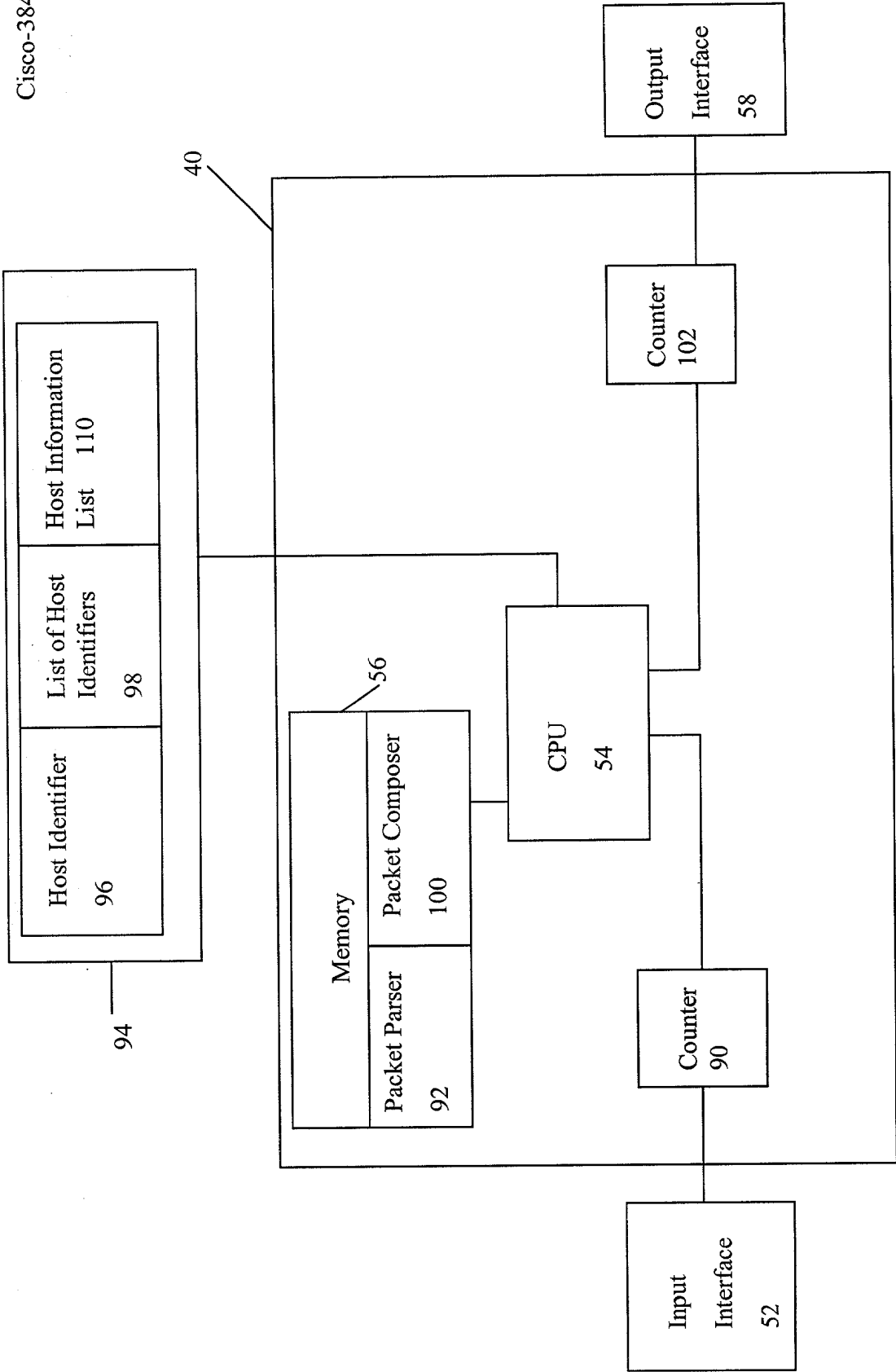


FIG. 5B

FIG. 6 is a flowchart illustrating a process for handling a data packet received from a host. The process begins with receiving a data packet from a host (60), then retrieving a host identifier (62). The host identifier is then matched against a list of host identifiers (64). If a match is found, the process maintains the state of authentication for the host (72), sets the giaddr field to the DHCP proxy address (74), and sets Option 82 in the options field of the data packet (86). The data packet is then forwarded to the address allocation device (80). If no match is found, the process drops or returns the data packet to the host (66) and maintains the state of unauthentication for the host (70). The process then receives a reply data packet from the address allocation device (82), sets the siaddr field to the DHCP proxy address (76), unflags Option 82 (88), and finally forwards the data packet to the host (84).

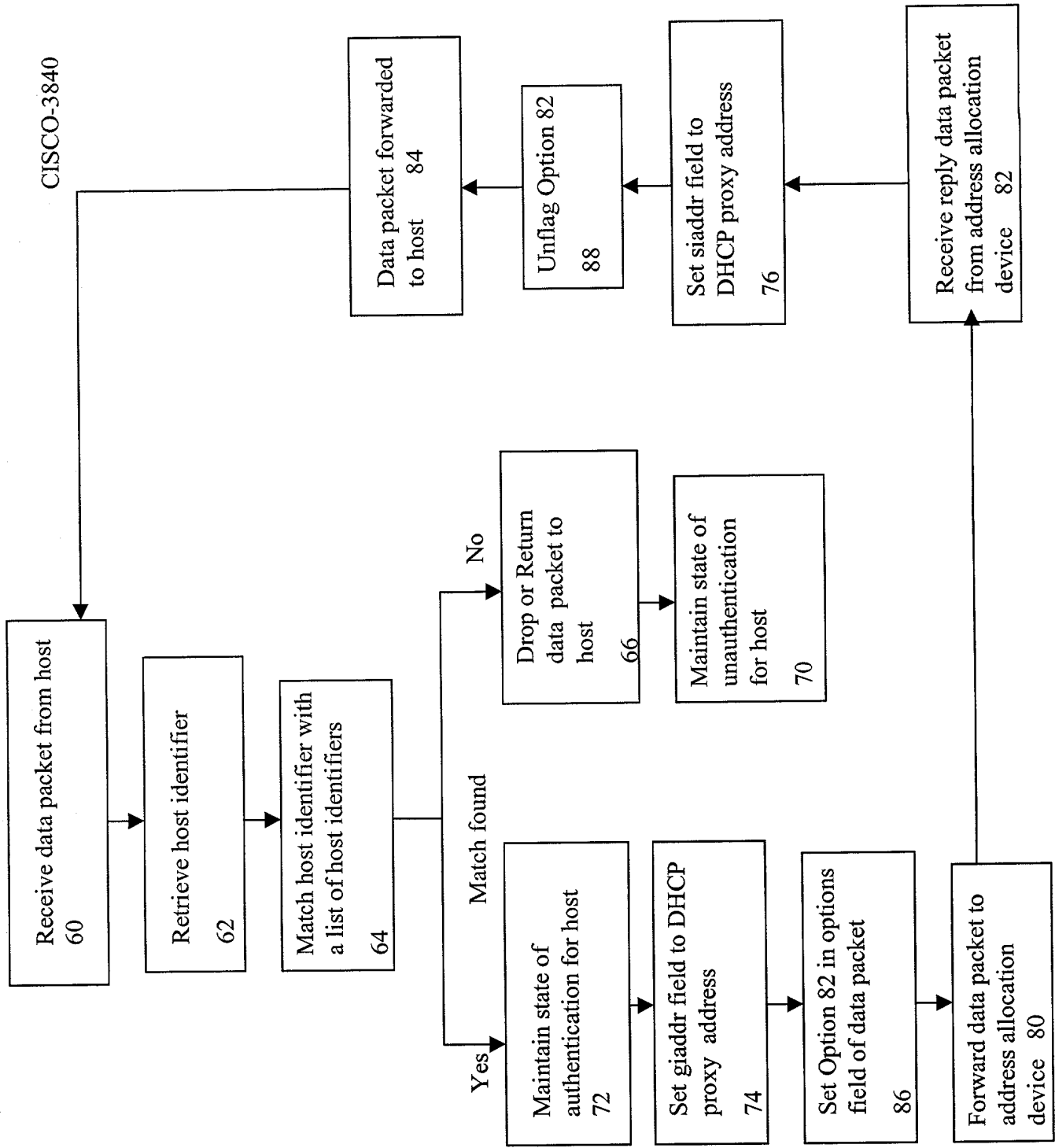


FIG. 6